Asian Journal of Applied Science and Technology (AJAST)
Volume 6, Issue 2, Pages 167-180, April-June 2022

Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions

Dr. Vinod Varma Vegesna

Sr. IT Security Risk Analyst, The Auto Club Group, United States of America. Email: vinodvarmava@gmail.com

DOI: http://doi.org/10.38177/ajast.2022.6217

Article Received: 28 February 2022 *Article Accepted: 29 May 2022* *Article Published: 30 June 2022*

ABSTRACT

Usually, cloud infrastructure is used individually by businesses, whereas the hybrid cloud would be a blend of two or many kinds of clouds. Because as clouds become increasingly common, safety issues also expanding. Because of such cybersecurity threats, numerous experts suggested procedures as well as ways to assure internet confidentiality. Providers of cloud-based services were accountable for the complete safety of cloud information. Nevertheless, since the clouds are accessible (easily accessible over the World wide web), much research has been conducted on cloud storage cybersecurity. This paper describes methods for enhancing security and reliability in decentralized cloud-based solutions, as well as suggests a few security solution methods of implementation.

Keywords: *Data integrity, Security solutions, Distributed cloud platform.*

1. Introduction

Cloud technology has now become ubiquitous. Throughout many situations, consumers were utilizing internet clouds without realizing them. Medium- and small-sized businesses may migrate towards cloud technology since that allows them faster accessibility for business applications while also lowering operational expenses [1]. Cloud services are more than just a technological response; it is additionally a working model wherein computer resources could be purchased or leased.

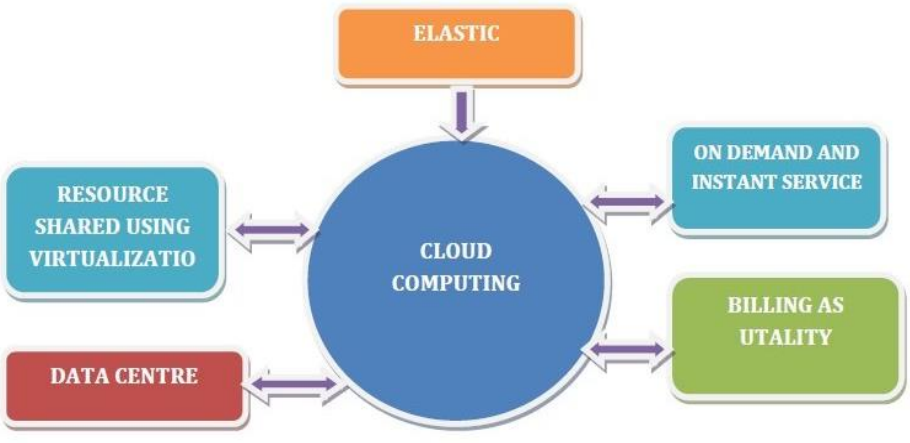

Figure 1. Simplified concept of cloud computing

The mission of cloud computing is to provide applications. Information from organizations is stored on the internet. Information assurance remains declining, but flexibility but also reactivity were rising. Businesses are becoming increasingly attempting to avoid concentrating on IT infrastructures. To boost productivity, companies must concentrate on their organizational processes. As a result, the overall relevance of cloud-based solutions keeps growing, only with the industry expanding massively with scientific or commercial groups paying attention to it. NIST defined cloud computing as a paradigm for solutions to solve, comfortable, on-demand network access to a

centralized pool of configurable computing resources (e.g., connections, data centers, memory, implementations, as well as utilities) which can be actively maximized but also issued with little integration management and engagement from telecommunications companies. Figure 1 depicts a simplified conceptual explanation of cloud-based solutions. As shown in Figure 2, the infrastructure paradigm is consisting of five basic features, 3 different models, and four different deployment models. Customers in this technique lease the information to a server located beyond company boundaries and overseen by a cloud operator. Memory, processors, connectivity, as well as capacity are also accessible through the network by a customer [2]. Cloud technology is made up of several techniques, including business architectures, configuration management, web 2.0, and several others.

Cloud technology raises several security problems. Nevertheless, enterprises need to have the cloud owing to the necessity for numerous capabilities to be utilized in high demand and an absence of adequate resources in order to meet the same need. Furthermore, cloud computing allows for very efficient information recovery as well as accessibility. Resources optimization is being handled by the cloud service provider.

1.1. Characteristics of Cloud Computing

Cloud services have several distinct properties. The initial is on-demand self-service, in which a service customer receives the capabilities they require that do not necessitate operator interaction or contact also with the cloud platform [3-5]. This same central characteristic is large network accessibility that implies that information may be accessible from almost anywhere using a conventional protocol using small or large companies with greater including a cellular telephone, notebook, or personal computer. An additional feature is capacity sharing that implies that facilities were aggregated to enabling over several users to utilize them. As in the multi-tenant model, resources are released continuously to a user, but once completed, they could well be transferred to the next to meet rising resource requirements. Even though customers were allocated to distributed resources, users need not understand where such capabilities are located. Companies might understand the location to a greater extent, including continent, region, and network infrastructure.

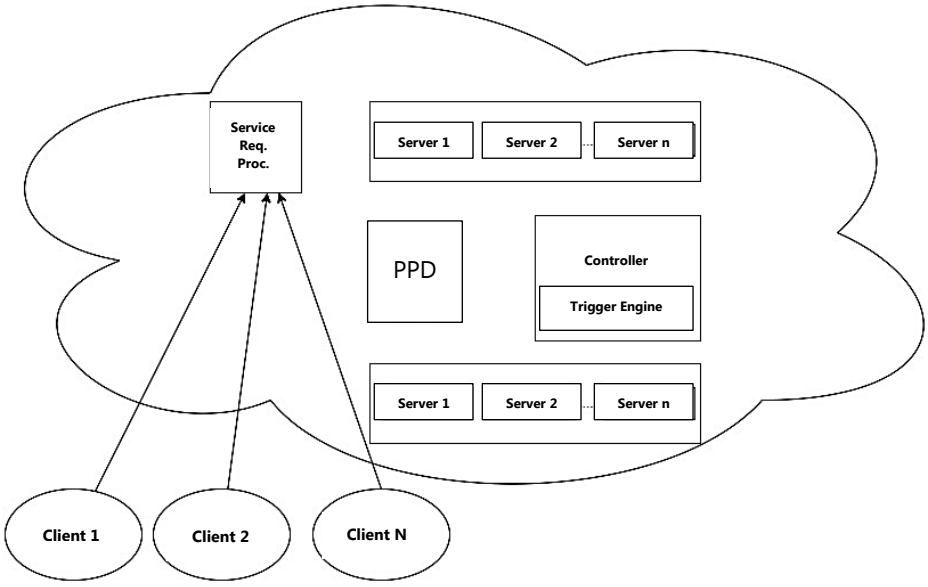

Figure 2. The architecture of a cloud environment

Quick flexibility seems to be another property of cloud applications that implies that resources are automatically raised whenever required as well as lowered when not. A quantified service is additionally one of the features which a customer requires to understand what amount is used. It is additionally necessary for the cloud vendor to understand the amount that the customer has utilized to bill them.

1.2. Service Models

There are three systems available. These features provided to the user vary across these variants. This could take the shape of technology, frameworks, or infrastructure. Table 1 compares the performance of such alternatives to the general framework.

Table 1. Assessment of cloud models to standard methods

S. No.	Conventional Models	Cloud Models
1.	**Applications** Client-side applications Client-server applications Web interface to local server applications Data and processes reside on PC or on local servers	**End-user cloud services** Rich internet applications Web 2.0 technologies Software-as-a-service Data and processes reside at the service provider
2.	**Developer tools & techniques** Client-side development tool Service-oriented architecture Composite applications Proprietary APIs	**App-component-as-a-service** Internet-hosted software services that enable mashups Web-hosted development tools Community development tools for shared templates and codes Proprietary service provider APIs
3.	**Middleware** App servers File and object stores Databases Integration servers	**Software-platform-as-services** Hosted app platform Hosted files, data, and object stores Hosted databases Software-integration-as-services

4.	**Physical Infrastructure** Severs Disks Network System management	**Virtual-infrastructure-as-services** Virtual servers Storage sharing VLAN Configuration Management-as-a-service

Software as a Service (SaaS) - Within that solution, the cloud-based service provider offers customers cloud-based software architecture such that they could utilize this for developing programs on the network infrastructure. Because users can indeed execute or consume such applications, they still did not influence the underlying technology as well as the physical environments of the clouds, including the networking, OS, as well as memory [6-11]. This provider of cloud services is now in control of managing multiple hardware settings but without customer interaction. The user may use an internet browser to connect to a program like a client application (Figure 3).

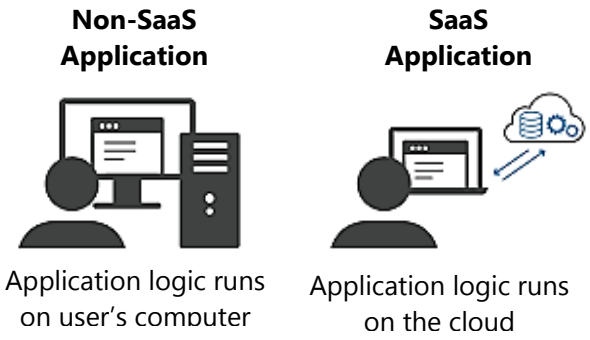

Figure 3. SaaS and non-SaaS models

Platform as a Service (PaaS) - Comparable to SaaS because the technology is managed mostly by cloud providers, however, this solution differs in that customers may install their own personal applications. Inside this architecture, customers may use the cloud platform company's application for downloading or distributing any own apps. Every cloud-based service provider controls or restricts issues, for example, although each user controls application settings.

IaaS (Infrastructure as a Service) - Computational resources including processors, memory, as well as networking could well be supplied using this application. Whatever random OS may be installed and used by an IaaS application. Users may indeed build or distribute apps upon the OS. Cloud solutions like Amazon EC2 are implementing similar strategies but also billing the customers on the number of resources used.

2. The Most Serious Threats to Cloud Computing

There are several concerns with cloud technology. Accidental deletions, information leakage, hostile hackers, the unsecured interface as well as APIs, user or security weaknesses, data location, but also denial of service are among the concerns highlighted. Figure 4 depicts the risks associated with using the cloud [12-14].

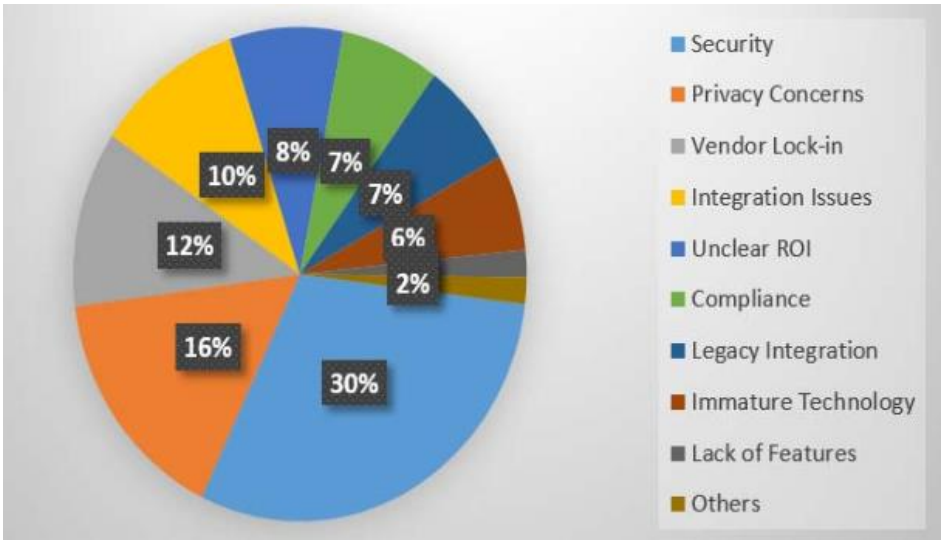

Figure 4. Possible Cloud computing threats

A. Loss of information

Businesses were transferring all of their sensitive information to cloud internet services. Considering the relatively inexpensive rates that the cloud provides, users must've been careful neither to disclose critical information to threats due to the numerous possibilities that could breach the information. The dangers in cloud technology were increasing as a result of hazards that seem to be unique to the internet which has not occurred in conventional devices, as well as difficulty in avoiding such vulnerabilities. There are various chances for information leakage because of a hostile assault, network breakdowns, or unintended erasure even by an operator lacking archives. Losses could be caused by natural disasters including an explosion or a catastrophe. Furthermore, whatever occurrence of damages its cryptographic keys may cause the loss of information. There are numerous ways recommended by CSA to secure the information:

- Using a robust API to ensure access.
- Encrypting and safeguarding information integrity as it travels through the route.
- Examining information security at operation and designing times.
- Adherence to strict key creation, storing, disposal, as well as standard operating procedures.
- Demanding that the provider delete any permanent multimedia content before pooling.
- Defining backups as well as recovery procedures.

B. Destruction of Data

A cloud infrastructure contains multiple users and businesses, all of which information is kept at the same location. Every compromise in this cloud infrastructure could disclose all individuals' and businesses' information. Users employing various apps on virtual servers may access the same databases because of multi-tenancy, as well as any damage incident that happens to it may impact users who utilize the same databases. Furthermore, SaaS companies also stated that their information is more secure compared to that of traditional suppliers.

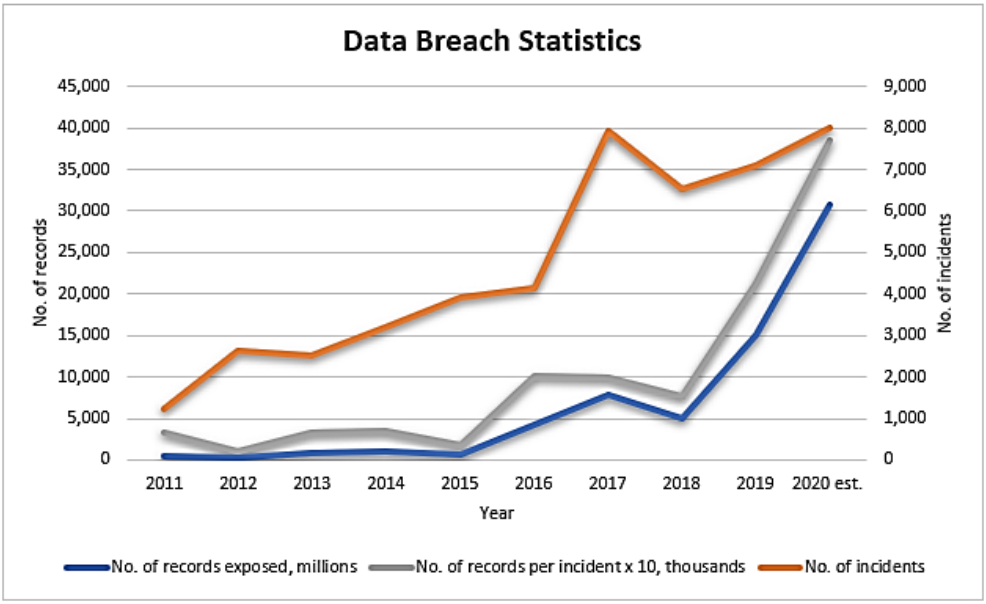

Figure 5. Increase in cybersecurity incidents in 2019

An insider may acquire data from a wide variety of methods; they can obtain information informally through obtaining a great deal of information on the clouds, as well as an event that might render the platform unsafe and therefore exposes users' information. According to the 2011 Data Breach Investigations Report, hacking and ransomware are among the most prevalent sources of security breaches, with 50% being phishing and 49% being ransomware. Figure 5 depicts the increase in data incidents in 2019.

C. Malicious Insiders

Malicious insiders are individuals who have access to sensitive information and therefore are allowed to administer it, including computer programmers or members of the business providing cloud-based services. Such individuals may acquire as well as destroy information whether they have been hired by many other firms or simply wish to harm a business. Although cloud computing providers could be unaware of this due to the incapacity to manage their personnel. CSA has presented several alternatives.

- Conducting detailed supplier performance and tightening management of supply chain ID.
- Promote a better understanding of human resource needs as a component of the legal arrangement.
- Increasing transparency in data protection as well as all software solution operations.
- Creating a procedure for notifying whenever privacy violations occur.

D. Insecure APIs and interfaces

The API is used to communicate seen between the cloud service provider and the client, allowing the customer to manage and supervise the information. As a result, such connections must be secured to prevent unauthorized access. When they are insufficient and the security features are incapable of defending these, it could result in resources being accessed even though they are strong passwords. CSA has several options for preventing unsafe interfaces as well as APIs:

- Examining the service company's defense in depth for interfacing.
- Ensuring effective identity management and security while transmitting data.
- Recognizing API interconnections.

E. Account or service theft

People accessed passwords to log in to cloud storage capabilities, therefore when their credentials are hacked or seized, the credentials were inevitably mishandled as well as changed. An unauthorized user with passwords may acquire the customers' information to acquire, modify, or destroy it, or even to market it to other individuals. Numerous ways are recommended by CSA to avoid accounts or security weaknesses:

- Preventing individuals from disclosing their identities.
- To use a two-factor authentication protocol.
- Monitoring all activity to identify unwanted entries.

F. Data Storage

Cloud companies have many data centers scattered around the globe. Data location is indeed a problem in cloud applications because cloud consumers have to understand exactly the information is hosted. Regardless of the jurisdiction, several nations compel corporations to retain user information in the nation. There are additional rules in various nations regarding which the corporation may keep its information. Additionally, information placement is essential whenever user information is housed inside an area prone to conflicts or calamities. Figure 6 depicts public views on cloud computing security.

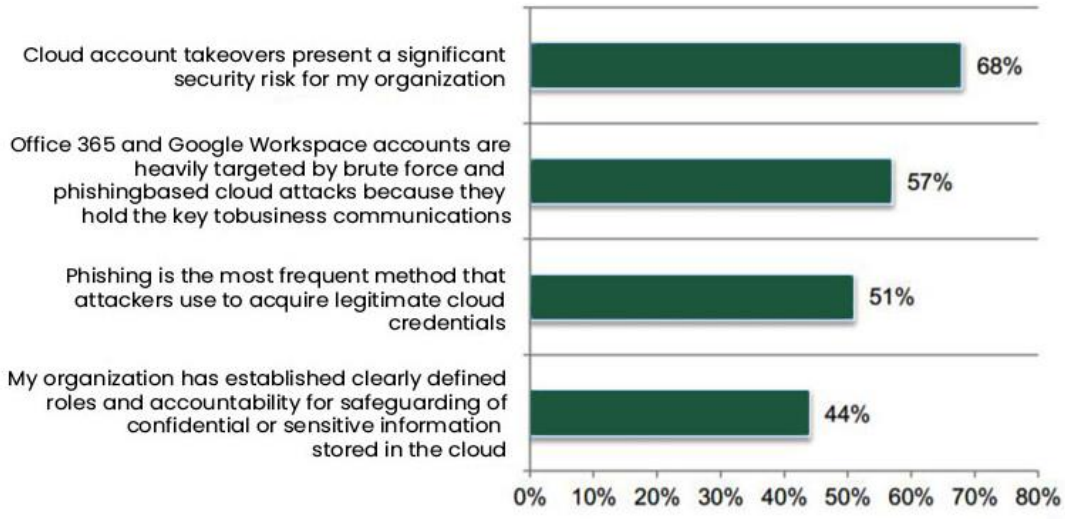

Figure 6. Cloud security perceptions

G. Denial of Service

Many companies want computer networks to remain readily available at all times since these major services businesses offer to rely on them. Such a provider of cloud-based services offers support that is pooled by several

customers. When an intruder consumes the resources, users will be unable to utilize them, resulting in a denial of service and perhaps slowing the availability of those resources. Users that use cloud computing and therefore are victimized by the network may indeed seek to interrupt the operation of these other companies.

2.1. Cloud Multi-tenancy

Multi-tenancy is seen as an essential factor in cloud computing by the CSA as well as ENISA. Nevertheless, despite the numerous advantages of multi-tenancy, there are several issues related to running over than single tenant solely on a single physical computer that is essential to leverage its architecture. Renters may assault each another as they reside in the same structure. Traditionally, any exploit might exist between two distinct physical machines; however, since 2 or even more renters share the very same infrastructure, an offender as well as victims could now exist within the same location. Figure 7 depicts the distinction between multi-tenancy and conventional situations. The technique is employed to isolate renters between them by constructing a virtual border for every client. Nevertheless, virtualization has a number of flaws.

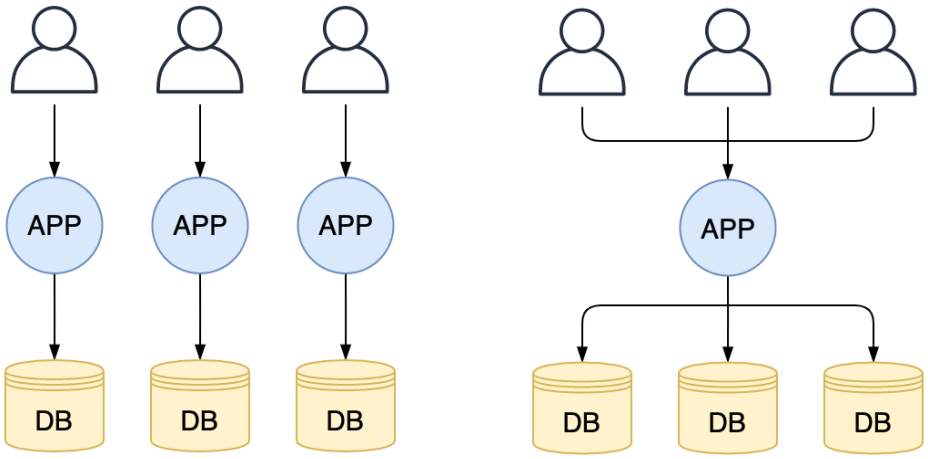

Figure 7. Traditional and Multi-Tenancy Cases

3. Review of Literature

Some of the methodologies for secured communication in cloud infrastructure are discussed here [15-18]. The researchers evaluated a multi-cloud system for data reliability as well as identity management. A multi-cloud architecture could provide multiple storage options. Therefore, reliability must be maintained. Numerous proven information access approaches have emerged for that purpose. For cloud-based solutions, the researchers reported Security as a Service instead. This suggested system handles audits as well as implements Service Level Agreements (SLAs) that are mutual contracts among cloud vendors and cloud consumers. Investigators presented a way for proving information assets with minimal proof ideas that might secure information integrity. Despite rigorous encryption techniques, this approach maximized throughput. Researchers contributed to a cryptographic algorithm that could be utilized to improve the security of cloud computing. Investigators provided a safe and adaptable architecture for improving cloud infrastructure.

The researchers also concentrated on multi-cloud storing challenges and offered a method for data integrity assurance. The approach is referred to as a proven management control system. Researchers helped to save

computer records which could be utilized to improve cloud-based services. The researchers developed a hardware-based way to prove information custody. This system ensures data integrity as well as timeliness. The researchers looked at safe information transfer in cloud-based solutions. They presented a paradigm provided by cloud integrity to do this. Cybersecurity - mediators used in a comparable type of activity. Clod information security is provided by the use of watermarking.

There is an excellent overview of numerous approaches to maintaining data security in a multi-cloud context. Remote Data Possession (RDP) with authorization was established for cloud information protection as well as flexibility. Researchers introduced a novel flavor of the PDP (O-PDP) method that employs 6-time complexity techniques in their PDP method. In addition to the capability to minimize data malpractices, the method is intended towards identifying damaged data or recovering damaged units.

To establish the concept of verifiable information privacy, researchers employed online codes (something of an erasing coding) in the manner that damaged information may be retrieved utilizing part of the encrypted information that was accessible. The system employs a mix of verifiable data possession as well as the encoding process. The researchers contend that the system was strong because two primary reasons. Users, as a consumer, may identify data degradation and retrieve damaged data.

The method consists of four phases pre-processing, task generation (clients), evidence of ownership (host), and validation (client). This study contributes to the safeguarding of leased information within the context of cloud-based solutions or any other kind of sourcing. The effectiveness of O-PDP pre-processing and trial time with each block size, as well as recognition rate versus frequency of requests blocks, are still the main outcomes of this study.

4. Assessment of The Security Model

4.1. Data Integrity Protection

Users of cloud environments often believe that if their data is protected before being transmitted to the clouds, that is safe. While cryptography offers excellent secrecy regarding cloud infrastructure attacks, it fails to protect the information from destruction done by technical indicators and application defects. There have been basically two methods for confirming the accuracy of data that has been leased to a distant server. A user or related parties may verify the authenticity of the information.

The first step is to obtain the file and thereafter verify the hash code. An asymmetric cryptographic coding technique is employed throughout this manner. MAC techniques use 2 parameters, a private key and a configurable piece of information, and create a single response, a MAC (tag). The procedure is therefore executed mostly on the user's computer. After obtaining a MAC, a data controller transfers the information into the cloud. The owner receives the data blocks, determines the MAC for it, and matches it to the one that was generated before contracting that information to ensure its authenticity.

This approach detects both unintentional as well as purposeful alterations. Furthermore, by utilizing the password, the information's validity is safeguarded, while only the person with the passcode may examine the information's

reliability and authenticity. Obtaining and computing the MAC of a huge document is a time-consuming yet difficult task. It is additionally inconvenient because it uses additional traffic. As a result, a simpler approach to determine its hash number is required.

The other is to use a hashing tree to calculate the hash code in the clouds. The hashing tree is formed from bottom to top with this approach, where the branches contain the information and the parent is indeed hashed till the roots are achieved. The database administrator only keeps the base. Whenever the owner wishes to double-check the information, he requests only the root value and matches it to the one that he possesses. This is not realistic to a certain degree since calculating the hash code of a large number of items uses additional processing. Whenever the given resource is only memory without processing, the client may download it as in the previous scenario, or transfer it to another third person, using additional capacity. As a result, a method for verifying information integrity yet conserving traffic and compute resources is required. Distributed data audits that investigate the information integrity or accuracy of distantly stored data have lately gained popularity.

A. Third-Party Auditor

A third-party auditor (TPA) is an individual who possesses the knowledge and competence to conduct certain audit work, as shown in Figure 8. The TPA system is employed to maintain integrity. Due to the number of events involving questionable acts, cloud service customers utilize third-party audits.

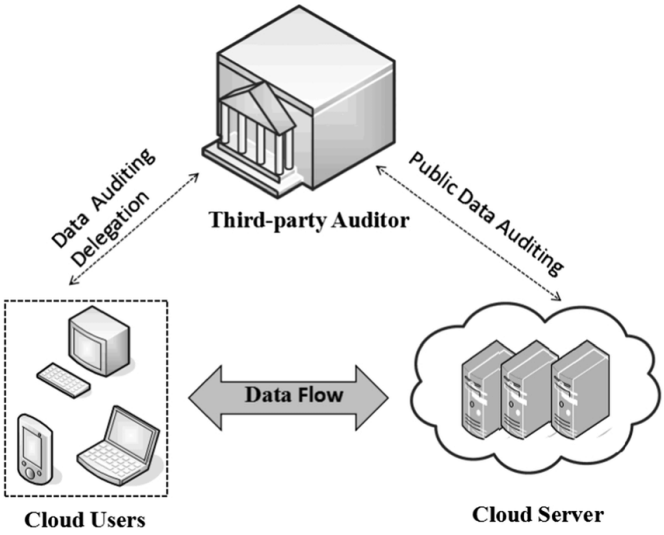

Figure 8. Third-party auditing infrastructure

The suggested approach ensures integrity as well as information protection for the data controller. The administrator is informed of all of his cloud systems. As a result, the technique ensures the information integrity of all owner's properties on the clouds. The information owner is involved in the audit work under this arrangement. To begin, TPA employs standard audit processes. When agents detect any modifications to the information, they inform the owner. To confirm such modifications, the administrator examines the auditing process records. If the owner feels that odd activities have occurred using their information, he may inspect it personally or have an additional audit appointed to them do so. As a result, the operator is constantly monitoring any changes to his personal information. There exists a set threshold that such a third-party examiner's answer must not surpass. All

adjustments that fall below or are equivalent to this level are validated by the data controller. Whereas if time surpasses that limit, the information owner will be obligated to do unexpected audits.

B. Provable Data Possession

This approach uses statistical demonstrations to verify ownership by randomly assigning a collection of frames out from servers. Researchers employed an RSA-based homomorphic verified tagging, whereby aggregates tagging to generate a communication that the customer may employ to establish that perhaps the servers possess a given item, irrespective no matter whether the user possesses accessibility or not to it. Regardless of the advantages of such a system, research failed to address dynamic memory storing, resulting in calculation and transmission delay inside the servers due to the complete file RSA numeration.

C. Methodology, Provider of Cloud Services & Authentication

Regular individuals and businesses that have information to keep on the internet and depend just on the network for information processing may both be examples of clients. A CSP manages and owns genuine cloud-based services and seems to have significant experience and resources in building and maintaining decentralized cloud service systems.

When asked, an additional TPA with expertise and skills which customers might not possess is entrusted to evaluate as well as expose the danger of cloud-based storage services in consumers' accounts. This study looks at the safety of cloud-based information storage that is effectively a decentralized backup system. A flexible and efficient decentralized infrastructure featuring explicit dynamic supporting documentation, encompassing blocks updating, deletion, and appending, has been proposed to ensure the correctness of client information stored in cloud-based data storage. Use erasure-correcting coding in document dissemination preparations to provide a redundant integrity vector and assure information trustworthiness.

They practically ensure the simultaneous identification of the offending server by integrating the homomorphic key with decentralized verification of erasure encrypted data. As per comprehensive security and speed testing, this solution is exceptionally effective and resistant to failure, malware change attacks, or even server collusion intrusions.

Various cloud elements often link to one another via applications programming interfaces, particularly cloud hosting, in the cloud environment, defined as the computer design of software products that are responsible for providing cloud applications. This is similar to the UNIX concept of having multiple programs each of which performs a particular task well enough and interacts with the others via global connections. The resultant technologies are much more controllable than monolithic equivalents since the complexities are managed.

A PKC-based homomorphic authenticator (e.g., a BLS signature or an RSA signature-based authenticator) is suggested to provide open integrity to the validation procedure. The main definition demonstrates this method using information dynamics assistance using a BLS-based strategy. The root hashing, in addition to the file set's total dimensions as well as component capacity, has now become the only item of data in the system that must originate from a reliable source. Any fragmentation may be checked by a user who merely has the root hashing of a

document set. It begins by determining the hashing of the block supplied to it. Since cloud services may manage multiple validation chances from various companies simultaneously, it becomes more practical to combine each of these patterns into a simple single one and validate it all simultaneously. This may be performed in a multiclient environment by enabling proven data changes and validation. Table 2 presents a comparison of several methods to cloud information security.

Table 2. Comparison of various approaches

Investigation	**Techniques**	**Explanations**	**Disadvantages**
Privacy preserved secure and dependable cloud data storage	MAC	Ensures data integrity	Not suitable for higher data files
Secured hash standard	Hash Algorithm	Stores the root hash of trees to authenticate received data	No assurance regarding the correctness of other outsourced data
Robust data security for cloud while using TPA	RSA, SHA-512	Design algorithm for data manipulations, insertion of records, and record deletions	If anyone deletes the records, this algorithm stops working
A secure index management scheme for providing data sharing in cloud storage	Proxy re-encryption	Identify the users accessing the records	-
Provable data possession at untrusted store	RSA-based homomorphic authenticator	Ensures possession of data files on unsecured memory	May leak user information to auditors, while using directly
Privacy-preserving public auditing for secure cloud storage	Random mask approach	Bilinear aggregate signatures, TPA performs multiple audit tasks simultaneously	-
Towards publicly auditable secure cloud data storage services	Proof of retrievability	A single key is utilized regardless of the size of the files	Needs higher resource costs for implementation

5. Conclusion

Cloud technology has proven to be one of the extremely successful implementations for the improvement of organizational performance. Because organizations have a significant amount of information to contain, cloud computing offers room to users by also allowing them to retrieve their information from anywhere at any moment in a simple manner. This paper suggests that enhanced utilization of cloud applications for information storage undoubtedly continues to increase the phenomenon of enhancing information storage methods inside the data center. Also, as individuals save their personally identifiable information as well as significant applications to the cloud, storing the information securely is becoming a major concern. This paper recommends that information stored in the cloud may be put at risk if not properly safeguarded. There are numerous existing techniques for effectively implementing protection in the cloud. This study offers an overview and discussion of cloud technology and security concerns, as well as strategies for strengthening cloud infrastructure encryption methods.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Consent for publication

Author declares that he/she consented for the publication of this research work.

References

[1] A. Aviram, S. Hu, B. Ford, and R. Gummadi (2010). Determinating timing channels in compute clouds. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Pages 103–108.

[2] A. Bessani, M. Correia, B. Quaresma, F. Andr´e, and P. Sousa (2013). Depsky: dependable and secure storage in a cloud-of-clouds. ACM Transactions on Storage (TOS), 9(4): 12.

[3] A. Corradi, M. Fanelli, and L. Foschini (2014). VM consolidation: A real case based on openstack cloud. Future Generation Computer Systems, 32: 118–12.

[4] Anil Lamba (2018). Protecting “cybersecurity & resiliency” of nation’s critical infrastructure - energy, oil & gas. International Journal of Current Research, 10(12): 76865–76876.

[5] S. Farné, F. Benzi, and E. Bassi (2020). IIoT Based Efficiency Optimization in Logistics Applications. Asian Journal of Basic Science & Research, 2(4): 59–73. doi: 10.38177/ajbsr.2020.2406.

[6] Satinderjeet Singh, Anil Lamba and Sivakumar Sai Rela Muni (2019). DSSE: distributed security shielded execution for communicable cyber threats analysis. International Journal of Current Research, 11(04): 3274–3282.

[7] Anil Lamba (2019). 8 Steps to Protect against Rising Third Party Cyber Risks. Cybernomics, 1(5): 29–31.

[8] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou (2012). Toward secure and dependable storage services in cloud computing. Services Computing, IEEE Transactions on, 5(2): 220–232.

[9] S. Alangari and N. Ahmed Khan (2021). Artificially Intelligent Warehouse Management System. Asian Journal of Basic Science & Research, 3(3): 16–24. doi: 10.38177/ajbsr.2021.3302.

[10] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng (2014). Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems, 25(2): 468–477.

[11] D. Catteddu (2010). Cloud computing: benefits, risks and recommendations for information security. In Web Application Security, Springer, Pages 17.

[12] Anil Lamba (2017). Deriving intelligent data analytics using anomaly detection framework for IoT network and smart environments. International Journal for Technological Research in Engineering, 4(6): 5682–5686.

[13] J.Rani & G.Glorinda (2021). A Simplified Fractal Texture Analysis Approach using Quadtree Decomposition with Huffman Coding Technique. Middle East Journal of Applied Science & Technology, 4(3): 01–09. doi: 10.46431/mejast.2021.4301.

[14] F. Zhang and H. Chen (2013). Security-preserving live migration of virtual machines in the cloud. Journal of Network and Systems Management, 21(4): 562–587.

[15] Anil Lamba (2015). A study paper on security related issue before adopting cloud computing service model. International Journal for Technological Research in Engineering, 3(4): 5837–5840.

[16] K. Pawar, C. Ambhika, and C. Murukesh (2021). IoT Hacking: Cyber Security Point of View. Asian Journal of Basic Science & Research, 3(2): 01–09. doi: 10.38177/ajbsr.2021.3201.

[17] G. Ateniese, R. Di Pietro, L. V. Mancini, G. Tsudik (2008). Scalable and efficient provable data possession. In Proceedings of the 4th international conference on Security and privacy in communication networks, Pages 9.

[18] G. Brunette, R. Mogull et al. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance, Pages 1–76.